



FortiToken Mobile 1.0 Administration Guide



FortiToken Mobile 1.0 Administration Guide

Revision 2

December 6, 2013

33-100-186424-20131206

Copyright© 2013 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

FortiToken Mobile Administration	4
Installing FortiToken Mobile tokens	4
Redemption certificate.....	4
“Virtual” certificate for free trial tokens	5
FortiToken Mobile installation.....	5
Provisioning and activating FortiToken Mobile tokens	6
FortiToken Mobile provisioning on a FortiGate unit.....	7
FortiToken Mobile provisioning on a FortiAuthenticator unit.....	8
FortiToken Mobile client activation.....	10
FortiToken Mobile token status	11

FortiToken Mobile Administration

To deploy your FortiToken Mobile tokens for One Time Password use by your end users, you must first install the tokens on your Authentication Server platform; either FortiGate running FortiOS 5.0 or greater, or FortiAuthenticator. After installing the tokens, you can assign them to your end users.

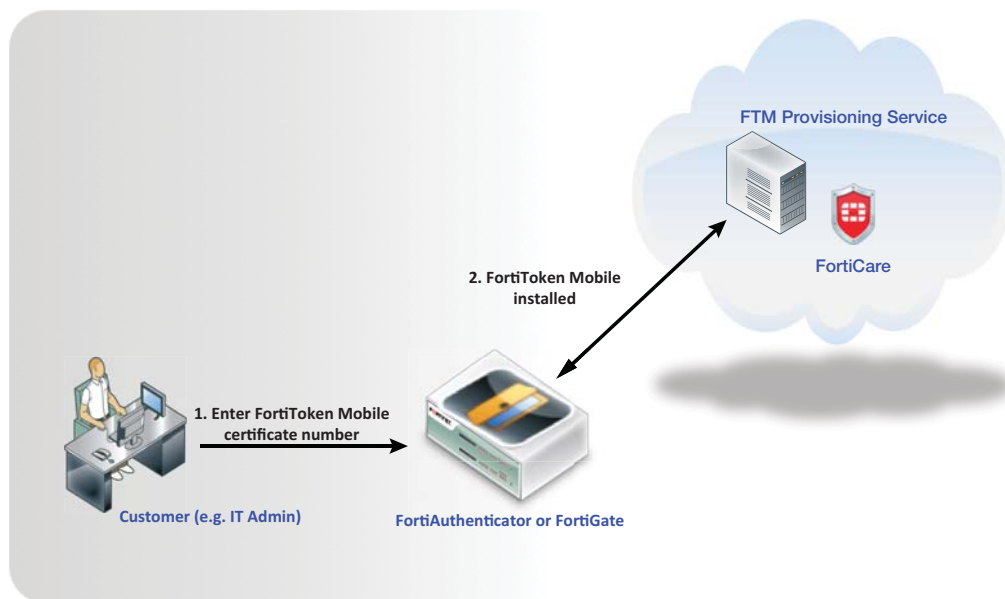
Installing FortiToken Mobile tokens

You will need a certificate code to install FortiToken Mobile tokens. There are two options for getting FortiToken Mobile token certificate codes for use on your authentication server; FortiToken Mobile Redemption Certificate, and FortiToken Mobile Free Trial “virtual” certificate.

The FortiToken Mobile installation process is the same for the Redemption Certificate and the Free Trial Tokens.

1. The authentication server administrator enters the certificate code.
2. The authentication server sends code to FortiToken Mobile provisioning server serial numbers, which validates the request, registers the FortiToken Mobile license and sends the FortiToken Mobile serial numbers back to the authentication server.

Figure 1: FortiToken Mobile installation context



Redemption certificate

For each FortiToken Mobile purchase, you will receive a redemption certificate for the number of tokens purchased. The activation code is 20 digits, revealed by scratching off the designated area of the certificate.

Figure 2: Sample redemption certificate for 200 FortiToken Mobile tokens



“Virtual” certificate for free trial tokens

Each FortiGate or FortiAuthenticator device comes with a trial license for two free trial tokens. The device must be registered with FortiCare to retrieve the tokens. The certificate code to use for the free trial FTM tokens is 0000-0000-0000-0000-0000.

FortiToken Mobile installation

To install the token on a FortiGate unit

1. Located the 20 digit code on the redemption certificate.
2. Login to the FortiGate Web-based manager.
3. Go to *User & Device > Two-factor Authentication > FortiToken* and select *Create New*.
4. Select *Mobile Token*.

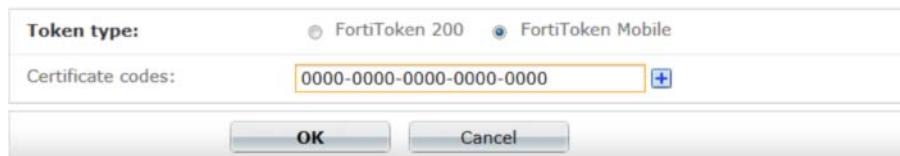
5. Enter the 20 digit certificate code in the *Activation Code* box.
6. Select *OK*.

Figure 3: Token list in FortiOS

Create New Edit Delete Refresh						
Type	Serial Number	Status	User	Drift	Comments	
	FTKMOB26BCF761D7	Available		0		
	FTKMOB26D4919224	Available		0		

To install the token on a FortiAuthenticator unit

1. Locate the 20 digit code on the redemption certificate.
2. Login to the FortiAuthenticator Web-based manager.
3. Go to Authentication > Local User Management > FortiTokens.
4. Select *Create New* and select *Mobile Token*.



The screenshot shows a web form for creating a new token. Under the 'Token type' section, 'FortiToken Mobile' is selected with a radio button. Below it, the 'Certificate codes' field contains the placeholder text '0000-0000-0000-0000-0000' and a blue plus icon to its right. At the bottom of the form are 'OK' and 'Cancel' buttons.

5. Enter the 20 digit certificate code in the *Activation Code* box
6. Select *OK*.

Figure 4: Token list in FortiAuthenticator



The screenshot shows a table of FortiTokens. The table has columns for Serial Number, Token Type, Status, Comment, User, and Drift. There are two rows of data, both showing 'FortiToken Mobile' with a status of 'Available' and a drift of '0'. The table is titled '2 FortiTokens'.

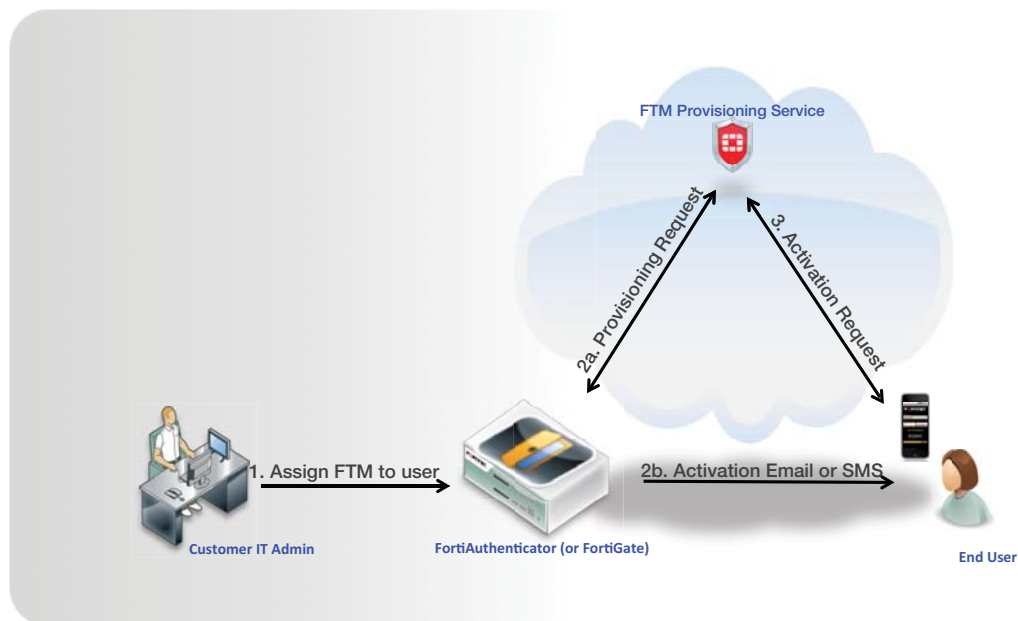
Serial Number	Token Type	Status	Comment	User	Drift
FTKMOB2A805D4724	FortiToken Mobile	Available			0
FTKMOB2A8CDF65CB	FortiToken Mobile	Available			0

Provisioning and activating FortiToken Mobile tokens

The FTM provisioning and activation operations include:

1. Authentication Server administrator has to first assign a FortiToken Mobile token to the user.
2.
 - a. The Authentication Server notifies the Provisioning Server that the token has been assigned for subsequent activation and receives back an activation code to forward to the end user
 - b. The end user receives an activation notification via email or SMS, depending on how the Authentication Server is configured.
3. After installing the FortiToken Mobile app on the mobile device, the end-user can activate the token anytime within a configurable provisioning time period.

Figure 5: Activating tokens



FortiToken Mobile provisioning on a FortiGate unit

To ensure messaging functions properly, configure the messaging servers, and configure users to receive messages from the server and use the FortiToken Mobile token.

To setup FortiToken Mobile provisioning

1. Go to *System > Config > Messaging Servers*.
2. Configure the servers as required.

Messaging Servers	
Email Service	
SMTP Server	<input type="text" value="mail.company.com"/>
Default Reply To	<input type="text" value="admin@company.com"/>
Authentication	<input checked="" type="checkbox"/> Enable
SMTP User	<input type="text" value="admin@company.com"/>
Password	<input type="password" value="....."/>
SMS Service	
<div>+ Create New ✎ Edit 🗑 Delete</div>	
Name	Address
No matching entries found	
<div>Apply</div>	

3. Go to *User & Device > User > User Definition*.

4. Select the user, or select *Create New*.

5. In *Contact Info*, select either the email address or phone number for SMS messages.
6. Select *Enable Two-factor Authentication* and select an available token.
7. Select *OK*.

The activation code will expire after a configurable period of time. To configure the time period, use the CLI command:

```
config system global
    set two-factor-ftm-expir <time-in-hours>
end
```

Note: The two-factor-ftm-expiry value should be in the range of 1-168.

Figure 6: Token assignment list

	User Name	Type	Two-factor Authentication	Ref.
<input type="checkbox"/>	guest	LOCAL		1
<input type="checkbox"/>	user1	LOCAL	FTKMOB26BCF761D7	0
<input type="checkbox"/>	user10	LOCAL		0
<input type="checkbox"/>	user15	LOCAL		1

FortiToken Mobile provisioning on a FortiAuthenticator unit

To ensure messaging functions properly, configure the messaging servers, and configure users to receive messages from the server and use the FortiToken Mobile token.

To setup FortiToken Mobile provisioning

1. Go to *System > Messages > SMTP Servers*, or *System > Messages > SMS Gateways*.
2. Configure the servers as required.

Name	Server	Default
Local Mail Server	localhost:25	
fortinet	mail.fortinet.com:25	<input checked="" type="checkbox"/>

3. Got to *Authentication > General > Options* and ensure the interval time period is set. The interval is the time period in hours in which the end user must activate the token before having to re-provision the token.

Lock-Out and Timeout Policies

Idle timeout for HTTP/HTTPS admin access: 5 minutes (1-480 mins)

E-mail/SMS token timeout: 60 seconds (10-3600s)

☒ Enable user account lock-out policy

Max. failed login attempts: 3

Lock-out period: 60 seconds (min. 60s)

User Password Complexity

Minimum length: 8

☒ Check for password complexity

User Password Change Policy

Maximum password age: 90 days (min. 14 days)

☒ Enforce password history

Number of passwords to remember: 3

FortiToken 200 Provisioning

Server address: update.fortiguard.net Server port: 443

FortiToken Mobile Provisioning

Activation timeout: 72 hours (min. 1 hour)

Server address: directregistration.fortinet.com Server port: 443

OK Cancel

4. Go to *Authentication > Local User Management > Local* or *Authentication > Local User Management > Remote*.
5. Select a user or select *Create New*.

Edit User

Username: user1

☐ Disabled

☒ Password-based authentication [Change Password]

☒ Token-based authentication

Deliver token code by: ☒ FortiToken ☐ E-mail ☐ SMS

FortiToken 200: [Please Select] FortiToken Mobile: FTKMOB2A805D4724

User Role

Role: ☐ Administrator ☒ User

☒ Allow RADIUS authentication

☐ Allow LDAP browsing

User Information

First name: Last name:

E-mail address: user1@company.com Phone number:

Mobile number: SMS gateway: Use default Test SMS

Street address:

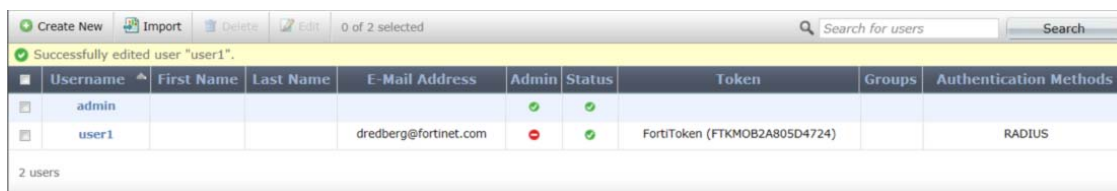
City: State/Province:

Country:

Password Recovery Options

6. In *User Information*, select either the email address or phone number for SMS messages.
7. Select select an available FortiToken Mobile token.
8. Select OK.

Figure 7: Token assignment list



	Username	First Name	Last Name	E-Mail Address	Admin	Status	Token	Groups	Authentication Methods
<input type="checkbox"/>	admin								
<input type="checkbox"/>	user1			dredberg@fortinet.com			FortiToken (FTKMOB2A805D4724)		RADIUS

2 users

FortiToken Mobile client activation

After successfully assigning a token to the end user, the end user will receive an activation notification as seen in the example below for email notification:

Welcome to FortiToken Mobile - One-Time-Password software token.

Please visit

<http://docs.fortinet.com/auth/FortiToken-Mobile-User-Guide-10.pdf>

for instructions on how to install your FortiToken Mobile application on your device and activate your token.

Your Activation Code, which you will need to enter on your device later, is "F9E801EB". You must activate your token by: Mon Oct 15 23:47:04 2012 GMT+00:00, after which you will need to contact your system administrator to re-enable your activation.

The end user must enter the 8 character activation code into the FortiToken Mobile app within the activation window given in the notification.

Figure 8: Activating the token



This will trigger an activation request to the provisioning server. If the request is valid, the FortiToken Mobile will be activated and ready to use on the mobile device.

FortiToken Mobile token status

The meanings of the three possible status values for FortiToken Mobile tokens are:

- Available: FortiToken Mobile token is available for provisioning
- Pending: FortiToken Mobile token is provisioned but not yet activated
- Assigned: FortiToken Mobile token is activated
- Locked: FortiToken Mobile tokens will be locked automatically if an Assigned token is Un-assigned when FortiCare FortiToken Mobile Provisioning Server is unreachable.
 - To unlock the locked token in FOS when FortiToken Mobile Provisioning Server is reachable, use the following CLI command:
`execute fortitoken-mobile renew <ftm-sn>`
 - To unlock the locked token in FortiAuthenticator, use the unlock button on the FortiToken user interface.

Figure 9: FortiToken Mobile Provisioning Status in FortiOS

Type	Serial Number	Status	User	Drift	Comments
	FTKMOB27A753D8CF	Locked		0	
	FTKMOB27ABEF2C	Available		0	
	FTKMOB27AFC834	Available		0	
	FTKMOB27B6442A15	Available		0	
	FTKMOB27BAAEC468	Available		0	
	FTKMOB27B8238C8	Available		0	
	FTKMOB27BDAEC66	Available		0	
	FTKMOB27C1C8106A	Available		0	
	FTKMOB27C7DCBEAD	Available		0	
	FTKMOB27C17407D4	Available		0	
	FTKMOB27CA553E18	Available		0	
	FTKMOB27CAB5C19	Available		0	
	FTKMOB27D1E28788	Available		0	
	FTKMOB27D9C14C8F	Available		0	
	FTKMOB27D8419F4	Available		0	
	FTKMOB27FA6F0E14	Available		0	
	FTKMOB271C890824	Available		0	
	FTKMOB273A8A8A76	Available		0	

Figure 10: FortiToken Mobile Provisioning Status in FortiAuthenticator

Serial Number	Token Type	Status	Comment	User	Drift
FTKMOB28046BA0A1	FortiToken Mobile	Pending		Local: user2	0
FTKMOB28103C38D6	FortiToken Mobile	Pending		Local: user1	0
FTKMOB28116FD4A4	FortiToken Mobile	Pending		Local: user3	0
FTKMOB2813439440	FortiToken Mobile	Available			0
FTKMOB2828145555	FortiToken Mobile	Available			0
FTKMOB28318517CB	FortiToken Mobile	Available			0
FTKMOB2837F8CCF4	FortiToken Mobile	Available			0
FTKMOB28392F3656	FortiToken Mobile	Available			0
FTKMOB28419AE3F5	FortiToken Mobile	Available			0
FTKMOB2858478335	FortiToken Mobile	Available			0
FTKMOB285ABF7C64	FortiToken Mobile	Available			0

